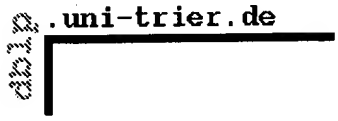

Jean-Jacques Quisquater

List of publications from the DBLP Bibliography Server - FAQ

Ask others: ACM DL - ACM Guide - CiteSeer - CSB - Google

Home Page

2003		
90	EE	Anand Raghunathan, Srivaths Ravi, Sunil Hattangady, Jean-Jacques Quisquater: Securing Mobile Appliances: New Challenges for the System Designer. DATE 2003: 10176-10183
89	EE	Mathieu Ciet, Tanja Lange, Francesco Sica, Jean-Jacques Quisquater: Improved Algorithms for Efficient Arithmetic on Elliptic Curves Using Fast Endomorphisms. EUROCRYPT 2003: 388-400
88	EE	Francois-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, Jean-Didier Legat: A methodology to implement block ciphers in reconfigurable hardware and its application to fast and compact AES RIJNDAEL. FPGA 2003: 216-224
87	EE	Gael Rouvroy, Francois-Xavier Standaert, Jean-Jacques Quisquater, Jean-Didier Legat: Design strategies and modified descriptions to optimize cipher FPGA implementations: fast and compact results for DES and triple-DES. FPGA 2003: 247
86	EE	Gael Rouvroy, Francois-Xavier Standaert, Jean-Jacques Quisquater, Jean-Didier Legat: Efficient FPGA Implementation of Block Cipher MISTY1. IPDPS 2003: 185
85	EE	Benoît Libert, Jean-Jacques Quisquater: Efficient revocation and threshold pairing based cryptosystems. PODC 2003: 163-171
84	EE	Gael Rouvroy, Francois-Xavier Standaert, Jean-Jacques Quisquater, Jean-Didier Legat: Efficient Uses of FPGAs for Implementations of DES and Its Experimental Linear Cryptanalysis. IEEE Transactions on Computers 52(4): 473-482 (2003)
2002		
83	EE	Jean-Jacques Quisquater: CHES: Past, Present, and Future. CHES 2002: 1
82	EE	Mathieu Ciet, Jean-Jacques Quisquater, Francesco Sica: Preventing Differential Analysis in GLV Elliptic Curve Scalar Multiplication. CHES 2002: 540-550
81	EE	Francois-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, Jean-Didier Legat: A Time-Memory Tradeoff Using Distinguished Points: New Analysis & FPGA Results. CHES 2002: 593-609
80	EE	Marc Joye, Jean-Jacques Quisquater, Sung-Ming Yen, Moti Yung: Observability Analysis - Detecting When Improved Cryptosystems Fail. CT-RSA 2002: 17-29
79	EE	Jean-Jacques Quisquater, Francois-Xavier Standaert, Gael Rouvroy, Jean-Pierre David, Jean-Didier Legat: A Cryptanalytic Time-Memory Tradeoff: First FPGA Implementation. FPL 2002: 780-789
		François Koeune, Gael Rouvroy, Francois-Xavier Standaert, Jean-Jacques Quisquater, Jean-

78	EE	Pierre David, Jean-Didier Legat: An FPGA Implementation of the Linear Cryptanalysis. FPL 2002: 845-852
77	EE	Francesco Sica, Mathieu Ciet, Jean-Jacques Quisquater: Analysis of the Gallant-Lambert-Vanstone Method Based on Efficient Endomorphisms: Elliptic and Hyperelliptic Curves. Selected Areas in Cryptography 2002: 21-36
2001		
76	EE	Emmanuel Bresson, Olivier Chevassut, David Pointcheval, Jean-Jacques Quisquater: Provably authenticated group Diffie-Hellman key exchange. ACM Conference on Computer and Communications Security 2001: 255-264
75	EE	Marc Joye, Jean-Jacques Quisquater: Hessian Elliptic Curves and Side-Channel Attacks. CHES 2001: 402-410
74	EE	Olivier Pereira, Jean-Jacques Quisquater: A Security Analysis of the Cliques Protocols Suites. CSFW 2001: 73-81
73	EE	Marc Joye, Jean-Jacques Quisquater, Moti Yung: On the Power of Misbehaving Adversaries and Security Analysis of the Original EPOC. CT-RSA 2001: 208-222
72	EE	Jean-Jacques Quisquater, David Samyde: ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. E-smart 2001: 200-210
71	EE	Werner Schindler, François Koeune, Jean-Jacques Quisquater: Improving Divide and Conquer Attacks against Cryptosystems by Better Error Detection / Correction Strategies. IMA Int. Conf. 2001: 245-267
70	EE	Marc Joye, Jean-Jacques Quisquater: On Rabin-Type Signatures. IMA Int. Conf. 2001: 99-113
69	EE	Mathieu Ciet, Jean-Jacques Quisquater, Francesco Sica: A Secure Family of Composite Finite Fields Suitable for Fast Implementation of Elliptic Curve Cryptography. INDOCRYPT 2001: 108-116
68		Olivier Pereira, Jean-Jacques Quisquater: Security Analysis of the Cliques Protocols Suites: First Results. SEC 2001: 151-166
67	EE	Louis C. Guillou, Michel Ugon, Jean-Jacques Quisquater: Cryptographic authentication protocols for smart cards. Computer Networks 36(4): 437-451 (2001)
66		Marc Joye, Jean-Jacques Quisquater, Tsuyoshi Takagi: How to Choose Secret Parameters for RSA-Type Cryptosystems over Elliptic Curves. Designs, Codes and Cryptography 23(3): 297-316 (2001)
2000		
65		Jean-Jacques Quisquater, Bruce Schneier: Smart Card Research and Applications, This International Conference, CARDIS '98, Louvain-la-Neuve, Belgium, September 14-16, 1998, Proceedings. Springer 2000
64		Gaël Hachez, François Koeune, Jean-Jacques Quisquater: Biometrics, Access Control, Smart Cards: A not so Simple Combination. CARDIS 2000: 273-288
63	EE	Gaël Hachez, Jean-Jacques Quisquater: Montgomery Exponentiation with no Final Subtractions: Improved Results. CHES 2000: 293-301
62	EE	Gaël Hachez, Laurent Den Hollander, Mehrdad Jalali, Jean-Jacques Quisquater, Christophe Vasserot: Towards a Practical Secure Framework for Mobile Code Commerce. ISW 2000: 164-178
1999		
		Xavier Verians, Jean-Didier Legat, Jean-Jacques Quisquater, Benoit M. Macq: A New

61	EE	Parallelism Management Scheme for Multiprocessor Systems. ACPC 1999: 246-256
60	EE	Tanguy Gilmont, Jean-Didier Legat, Jean-Jacques Quisquater: Enhancing Security in the Memory Management Unit. EUROMICRO 1999: 1449-
59	EE	Xavier Verians, Jean-Didier Legat, Jean-Jacques Quisquater, Benoit M. Macq: A Graph-Oriented Task Manager for Small Multiprocessor Systems. Euro-Par 1999: 735-744
58		Julien P. Stern, Gaël Hachez, François Koeune, Jean-Jacques Quisquater: Robust Object Watermarking: Application to Code. Information Hiding 1999: 368-378
57		Yvo Desmedt, Tri Van Le, Jean-Jacques Quisquater: Nonbinary Audio Cryptography. Information Hiding 1999: 478-489
56	EE	Jean-Marie Kabasele-Tenday, Jean-Jacques Quisquater, Marc Lobelle: Deriving a Role-Based Access Control Model from the OBBAC Model. WETICE 1999: 147-151
55	EE	H. Massias, X. Serret Avila, Jean-Jacques Quisquater: Timestamps: Main Issues on Their Use and Implementation. WETICE 1999: 178-183
54	EE	Marc Joye, Arjen K. Lenstra, Jean-Jacques Quisquater: Chinese Remaindering Based Cryptosystems in the Presence of Faults. Journal of Cryptology 12(4): 241-245 (1999)
1998		
53		Jean-Jacques Quisquater, Yves Deswarte, Catherine Meadows, Dieter Gollmann: Computer Security - ESORICS 98, 5th European Symposium on Research in Computer Security, Louvain-la-Neuve, Belgium, September 16-18, 1998, Proceedings. Springer 1998
52	EE	Yvo Desmedt, Shuang Hou, Jean-Jacques Quisquater: Audio and Optical Cryptography. ASIACRYPT 1998: 392-404
51		Jean-François Dhem, François Koeune, Philippe-Alexandre Leroux, Patrick Mestré, Jean-Jacques Quisquater, Jean-Louis Willems: A Practical Implementation of the Timing Attack. CARDIS 1998: 167-182
50		Jean-François Dhem, Jean-Jacques Quisquater: Recent Results on Modular Multiplications for Smart Cards. CARDIS 1998: 336-352
49		Gérard Eizenberg, Jean-Jacques Quisquater: Panel Session: Watermarking. ESORICS 1998: 275
48	EE	Yvo Desmedt, Shuang Hou, Jean-Jacques Quisquater: Cerebral Cryptography. Information Hiding 1998: 62-72
47	EE	V. Darmstaedter, Jean-Francois Delaigle, Jean-Jacques Quisquater, Benoit M. Macq: Low cost spatial watermarking. Computers & Graphics 22(4): 417-424 (1998)
46		Marc Joye, Jean-Jacques Quisquater: Reducing the Elliptic Curve Cryptosystem of Meyer-Müuller to the Cryptosystem of Rabin-Williams. Designs, Codes and Cryptography 14(1): 53-56 (1998)
45	EE	Henri Gilbert, Dipankar Gupta, Andrew M. Odlyzko, Jean-Jacques Quisquater: Attacks on Shamir's `RSA for Paranoids'. Information Processing Letters 68(4): 197-199 (1998)
1997		
44	EE	Marc Joye, Jean-Jacques Quisquater: On the Importance of Securing Your Bins: The Garbage-man-in-the-middle Attack. ACM Conference on Computer and Communications Security 1997: 135-141
43		Jean-Francois Delaigle, Christophe De Vleeschouwer, Francois Goffin, Benoit M. Macq, Jean-Jacques Quisquater: Low Cost Watermarking Based on a Human Vision Model. ECMAST 1997: 153-167

42		Daniel Bleichenbacher, Marc Joye, Jean-Jacques Quisquater: A new and optimal chosen-message attack on RSA-type cryptosystems. ICICS 1997: 302-313
41		Marc Joye, Jean-Jacques Quisquater, Feng Bao, Robert H. Deng: RSA-type Signatures in the Presence of Transient Faults. IMA Int. Conf. 1997: 155-160
40		Francois Goffin, Jean-Francois Delaigle, Christophe De Vleeschouwer, Benoit M. Macq, Jean-Jacques Quisquater: Low-Cost Perceptive Digital Picture Watermarking Method. Storage and Retrieval for Image and Video Databases (SPIE) 1997: 264-277
39		Jean-Jacques Quisquater, Benoit M. Macq, Marc Joye, N. Degand, A. Bernard: Practical Solution to Authentication of Images with a Secure Camera. Storage and Retrieval for Image and Video Databases (SPIE) 1997: 290-297
1996		
38		Gérard Eizenberg, Dominique Gonthier, Alistair Kelman, Jean-Jacques Quisquater: Authors' Rights and Copyright Protection. ESORICS 1996: 324
37		Marc Joye, Jean-Jacques Quisquater: Protocol Failures for RSA-Like Functions Using Lucas Sequences and Elliptic Curves. Security Protocols Workshop 1996: 93-100
1995		
36		Louis C. Guillou, Jean-Jacques Quisquater: Advances in Cryptology - EUROCRYPT '95, International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21-25, 1995, Proceeding. Springer 1995
35		J.-M. Boucqueau, S. Lacroix, Benoit M. Macq, Jean-Jacques Quisquater: Equitable Conditional Access and Copyright Protection for Image Based on Trusted Third Parties. COST 237 Workshop 1995: 229-243
34	EE	Philippe Béguin, Jean-Jacques Quisquater: Fast Server-Aided RSA Signatures Secure Against Active Attacks. CRYPTO 1995: 57-69
1994		
33		Philippe Béguin, Jean-Jacques Quisquater: Secure Acceleration of DSS Signatures Using Insecure Server. ASIACRYPT 1994: 249-259
32	EE	Olivier Delos, Jean-Jacques Quisquater: An Identity-Based Signature Scheme with Bounded Life-Span. CRYPTO 1994: 83-94
1993		
31		Olivier Delos, Jean-Jacques Quisquater: Efficient multi-signature schemes for cooperating entities. Algebraic Coding 1993: 63-74
1992		
30		Yves Deswarte, Gérard Eizenberg, Jean-Jacques Quisquater: Computer Security - ESORICS 92, Second European Symposium on Research in Computer Security, Toulouse, France, November 23-25, 1992, Proceedings. Springer 1992
29	EE	Jean-Claude Bermond, Charles Delorme, Jean-Jacques Quisquater: Table of Large (*Delta, D*)-Graphs. Discrete Applied Mathematics 37/38: 575-577 (1992)
28		Jean-Claude Bermond, Pavol Hell, Jean-Jacques Quisquater: Construction of Large Packet Radio Networks. Parallel Processing Letters 2: 3-12 (1992)
1991		
27		Dominique de Waleffe, Jean-Jacques Quisquater: Better Login Protocols for Computer Networks. Computer Security and Industrial Cryptography 1991: 50-70

26		Jean-Jacques Quisquater, Yvo Desmedt: Chinese Lotto as an Exhaustive Code-Breaking Machine. IEEE Computer 24(11): 14-22 (1991)
25		Samy Bengio, Gilles Brassard, Yvo Desmedt, Claude Goutier, Jean-Jacques Quisquater: Secure Implementations of Identification Systems. Journal of Cryptology 4(3): 175-183 (1991)
1990		
24		Jean-Jacques Quisquater, Joos Vandewalle: Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings. Springer 1990
23	EE	Dominique de Waleffe, Jean-Jacques Quisquater: CORSAIR: A SMART Card for Public Key Cryptosystems. CRYPTO 1990: 502-513
22	EE	Louis C. Guillou, Jean-Jacques Quisquater, Michael Walker, Peter Landrock, Caroline Shafer: Precautions Taken Against Various Potential Attacks in ISO/IEC DIS 9796 "Digital Signature Scheme Giving Message Recovery". EUROCRYPT 1990: 465-473
1989		
21	EE	Marijke De Soete, Jean-Jacques Quisquater, Klaus Vedder: A Signature with Shared Verification Scheme. CRYPTO 1989: 253-262
20	EE	Jean-Jacques Quisquater, Jean-Paul Delescaille: How Easy is Collision Search. New Results and Applications to DES. CRYPTO 1989: 408-413
19	EE	Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis C. Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, Soazig Guillou, Thomas A. Berson: How to Explain Zero-Knowledge Protocols to Your Children. CRYPTO 1989: 628-631
18	EE	Jean-Jacques Quisquater, Marc Girault: 2n-Bit Hash-Functions Using n-Bit Symmetric Block Cipher Algorithms. EUROCRYPT 1989: 102-109
17	EE	Jean-Jacques Quisquater, Jean-Paul Delescaille: How Easy is Collision Search? Application to DES (Extended Summary). EUROCRYPT 1989: 429-434
16	EE	Jean-Jacques Quisquater, André Bouckaert: Zero-Knowledge Procedures for Confidential Access to Medical Records (Extended Summary). EUROCRYPT 1989: 662-664
1988		
15	EE	Louis C. Guillou, Jean-Jacques Quisquater: A "Paradoxical" Indentity-Based Signature Scheme Resulting from Zero-Knowledge. CRYPTO 1988: 216-231
14	EE	Louis C. Guillou, Jean-Jacques Quisquater: A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Trasmission and Memory. EUROCRYPT 1988: 123-128
1987		
13	EE	Jean-Jacques Quisquater: Secret Distribution of Keys for Public-Key Systems. CRYPTO 1987: 203-208
12	EE	Louis C. Guillou, Jean-Jacques Quisquater: Efficient Digital Public-Key Signature with Shadow (Abstract). CRYPTO 1987: 223
11	EE	Jean-Jacques Quisquater, Jean-Paul Delescaille: Other Cycling Tests for DES (Abstract). CRYPTO 1987: 255-256
1986		
10	EE	Yvo Desmedt, Jean-Jacques Quisquater: Public-Key Systems Based on the Difficulty of

		Tampering (Is There a Difference Between DES and RSA?). CRYPTO 1986: 111-117
9		Yvo Desmedt, Frank Hoornaert, Jean-Jacques Quisquater: Several Exhaustive Key Search Machines and DES. EUROCRYPT 1986: 17-19
8		Jean-Claude Bermond, Charles Delorme, Jean-Jacques Quisquater: Strategies for Interconnection Networks: Some Methods from Graph Theory. Journal of Parallel and Distributed Computing 3(4): 433-449 (1986)
1985		
7	EE	Jean-Jacques Quisquater, Yvo Desmedt, Marc Davio: The Importance of "Good" Key Scheduling Schemes (How to Make a Secure DES Scheme with <= 48 Bit Keys). CRYPTO 1985: 537-542
1984		
6	EE	Marc Davio, Yvo Desmedt, Jo Goubert, Frank Hoornaert, Jean-Jacques Quisquater: Efficient Hardware and Software Implementations for the DES. CRYPTO 1984: 144-146
5	EE	Yvo Desmedt, Jean-Jacques Quisquater, Marc Davio: Dependence of Output on Input in DES: Small Avalanche Characteristics. CRYPTO 1984: 359-376
4	EE	Marc Davio, Yvo Desmedt, Jean-Jacques Quisquater: Propagation Characteristics of the DES. EUROCRYPT 1984: 62-73
1983		
3		Marc Davio, Yvo Desmedt, Marc Fosseprez, René Govaerts, Jan Hulsbosch, Patrik Neutjens, Philippe Piret, Jean-Jacques Quisquater, Joos Vandewalle, Pascal Wouters: Analytical Characteristics of the DES. CRYPTO 1983: 171-202
1982		
2		Jean-Claude Bermond, Charles Delorme, Jean-Jacques Quisquater: Tables of Large Graphs with Given Degree and Diameter. Information Processing Letters 15(1): 10-13 (1982)
1973		
1		Philippe Delsarte, Jean-Jacques Quisquater: Permutation Cascades with Normalized Cells. Information and Control 23(4): 344-356 (1973)

Google Advanced Search Preferences Language Tools Search Tips

multiprocessor security computer Google Search

Web · Images · Groups · Directory · News

Searched the web for multiprocessor security computer crypto. Results 1 - 10 of about 1,760. Search took 0.2

Eivom.com - **Computer** Help Index - topics beginning with S & T - ...
... of Personal Computers | **Computer** Cops | Daily ... Lifecycle | MSDN Library | **Multiprocessor**
Workstation Glossary ... up Patching | RouterGod | **Security** News Portal ...
www.eivom.com/Computing/comhelpst.htm - 86k - Cached - Similar pages

DBLP: Jean-Jacques Quisquater
... A Graph-Oriented Task Manager for Small **Multiprocessor** Systems. ... **CRYPTO** 1994: 83-94. ... Gérard Eizenberg, Jean-Jacques Quisquater: **Computer Security** - ESORICS 92 ...
www.informatik.uni-trier.de/~ley/db/indices/ a-tree/q/Quisquater:Jean=Jacques.html - 43k - Oct 21, 2003 - Cached - Similar pages

[PPT] Adventures in **Computer Security**
File Format: Microsoft Powerpoint 97 - View as HTML
... Shared memory **multiprocessor**. ... Hope to encourage additional operating system **security** research. ... DoD Trusted **Computer** Sys Evaluation Criteria (Orange Book). ...
crypto.stanford.edu/cs155/lecture9.ppt - Similar pages

News Item: **crypto**\o&r\appendix
www.swiss.ai.mit.edu/6805/articles/ crypto/nrc-report/28ea.html - 18k - Cached - Similar pages

computercollectief over UNIX Clones
... on the path of advanced **multiprocessor** and application ... for administrators to define system **security** policies ... **computer**/processor, minimaal 80386-processor, Pentium ...
www.comcol.nl/idx.php?anr=7606g - 29k - Oct 21, 2003 - Cached - Similar pages

Information **Security** Magazine
... as a fast PCI bus on a Sun **computer**) means that ... beyond the capacity of even the biggest **multiprocessor** systems on ... SSL is a user-to-application **security** protocol ...
www.infosecuritymag.com/articles/january00/cover.shtml - 46k - Cached - Similar pages

Bibliography
... Integrating **security** with fault-tolerant distributed databases. ... Lecture Notes in **Computer** Science 293 ... How to make a **multiprocessor computer** that correctly ...
www.julienstern.org/files/ida/node14.html - 8k - Cached - Similar pages

Dan Wallach / Comp 620: Seminar in Secure Systems
... HYDRA: The kernel of a **multiprocessor** operating system ... some nice links collected for **c mputer security** and cryptography ... a large collection of **crypt** and **security** ...
www.cs.rice.edu/~dwallach/courses/ comp620_f98/papers.html - 14k - Cached - Similar pages

Archiv1_e
... W. Adi: Basics of Data **Security** in Digital ... W. Adi: Basics of Error Control in **C mputer**

Systems, 1984 ... management for the design of a **multipr cessor** ASICs for ...
www.ida.ing.tu-bs.de/people/adi/Archiv1_e.shtml - 13k - Oct 21, 2003 - Cached - Similar pages

E-Commerce News: RSA Expands E-Commerce **Security** Lineup
... In other online **security**-related news, a US ... heels of the Clinton administration's revised **crypt** export policy ... free speech issues and a **c mputer** programmer who ...
www.ecommercetimes.com/perl/story/2385.html - 39k - Oct 21, 2003 - Cached - Similar pages

Gooooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

multiprocessor security computer Google Search Search within results

Dissatisfied with your search results? Help us improve.

Google Home - Advertise with Us - Business Solutions - Services & Tools - Jobs, Press, & Help